

S/MIME Interoperability

Dale Walters
NIST-ITL
Security Division
301 975-3641
walters@csmes.ncsl.nist.gov

S/MIME Interoperability

- The S/MIME Specification
- The NIST S/MIME Interoperability Laboratory
- S/MIME Interoperability Testing
 - What we have done thus far
 - What we learned
 - What we intend to do in the future

The S/MIME Specification

- RFC822 Specification for electronic mail developed in early 1980's
- Multipurpose Internet Mail Extension (MIME) was developed by the IETF to support non-textual data
- The S/MIME specification is an extension of the MIME standard to support an encryption and Digital Signature service
 - Developed by a group of vendors led by RSA
 - version 2 currently deployed
 - version 3 being standardized by IETF

The S/MIME Specification

- Allows different symmetric encryption algorithms (DES, Triple-DES, RC2)
- Version 2 requires RSA Public Key Technology
- Uses PKCS#7 to specify the content and form of information required to provide a digital signature service
- Supports two data signing formats
 - *clear*
 - *opaque*

The NIST S/MIME Interoperability Laboratory

- Baltimore Technologies

- UNICERT CA (2.11) /ISOCOR Dir.
- Registration Authority
- Mail Secure Clients
 - Plug-in to Microsoft Exchange

- World Talk

- World Secure Clients (3.0)
 - Plug-in to Microsoft Exchange
 - Plug-in to Eudora

The NIST S/MIME Interoperability Laboratory

● Netscape

- Netscape Administrator Server
- Netscape Certificate Server (1.01)
- Netscape Directory Server (4.0)
- Netscape Communicator (4.5)
 - Netscape Messenger

● Microsoft

- Microsoft Outlook Express client (2000)
- Microsoft Exchange Server (5.5)
- Microsoft Windows 2000 (NT5)

The NIST S/MIME Interoperability Laboratory

● Entrust

- Entrust Manager/Administrator (3.0c)
- Entrust Directory (ICL i500 DSA 6.4.3)
- Entrust Express 4.0 (Plug-in for Eudora mail client)

● Spyrus

- S2 Certificate Authority
- ORA 1.2
- Smart Card Readers

What We Learned

- There are still significant barriers to interoperability
 - Inability to process both clear and opaque messages
 - Dependence on certificates issued by a particular CA
 - Inability to publish or retrieve certificates from a certificate repository
 - Inability to extend knowledge about certificate revocation beyond a single vendors products

What We Learned

- Some S/MIME applications support multiple certificates for a single user. Some don't
- Some applications provide the ability to trust self-signed certificates. Some don't
- Certificate Authorities can be implemented with different architectures
- The documentation for configuring the Certificate servers and Directory servers needs to be improved
- Algorithm support did not cause interoperability problems except by design (export vs. non-export versions)

The Future

- Integrate Entrust, Microsoft, Spyrus, and Netscape Servers and S/MIME clients in our Lab
- Test with other Federal Agencies
- Test with these and other vendors if there is Interest